Deterring Iran's Use of Offensive Cyber:

A Case Study

Michael Connell

October 2014

CNA
ANALYSIS & SOLUTIONS

Distribution unlimited

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Deterring Iran's Use of Offensive Cyber: A Case Study	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **CNA Analysis & Solutions,3003 Washington Boulevard,Arlington,VA,22201**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

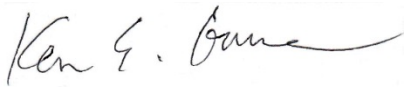
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**24**	

This document contains the best opinion of CNA at the time of issue.
It does not necessarily represent the opinion of the sponsor.

Distribution

Distribution unlimited. Specific authority: N00014-11-D-0323.

Approved by: **October 2014**



Ken E. Gause, Director
International Affairs Group
Center for Strategic Studies

Executive summary

Since 2011, Iran and the United States have been engaged in a low-level cyber conflict. Iranian cyber forces and cyber proxies have launched distributed denial of service (DDoS), web defacement, spear phishing, and data manipulation attacks against U.S. and allied banks, media outlets, government offices, social networking sites, and military communications networks. These attacks pose critical questions for U.S. entities with cyber roles and missions. Can Iran be deterred from engaging in offensive cyber? If so, how? What would a deterrence strategy that targets Iran's use of offensive cyber look like? This paper explores how the concept of tailored deterrence could be applied to Iran in the cyber sphere. Utilizing a case-studies approach, it analyzes some of the unique features associated with the regime's political and military decision making processes, how its cyber programs and entities are structured and affiliated with the regime, the TTP that these entities employ, their relative capabilities, and how these factors could play in a cyber-deterrence scenario.

Its key findings include the following:

- Iranian cyber capabilities are modest but growing. Prior to 2012, the tactics employed by Iran's cyber forces and their proxies were fairly basic by hacking standards—mainly DDoS attacks with botnets and DNS hijackings and recursions. More recent activities by Iranian cyber forces and their proxies—including a massive cyber attack on Saudi Aramco, the penetration the Navy Marine Corps Intranet (NMCI), and a social engineering operation dubbed "Newscaster"—indicate that Iran cyber efforts are maturing and becoming more systematic.

- Iranian officials are likely to define offensive cyber differently than we do. Given the regime's sensitivities to perceived internal meddling and Western soft power projection, attempts to facilitate information flow into Iran could be regarded as a form of offensive cyber.

- The fractious nature of the Iranian political system potentially raises the risk of escalation and complicates U.S. response options in a cyber environment.

- Cyber attacks on Iran's nuclear and commercial infrastructure, coupled with Western attempts to widen the information aperture into Iran, have raised the suspicions of the regime and convinced many Iranian officials that the Islamic Republic is the victim of cyber aggression by the United States and Israel.

- Iran's use of cyber proxies, while hardly unique, adds another layer of complexity to the problem of attribution. It also could have unintended consequences in terms of escalation management, particularly in a crisis.

- As part of a strategy that is tailored to deter Tehran's use of offensive cyber Washington should:

  - Define what categories of activities in the cyber realm it considers intolerable and would therefore warrant retaliation, and communicate its intent to Iran's leadership via multiple channels.

  - Demonstrate that it has a credible means of retaliation in cyberspace, while at the same time declaring that it reserves the right to retaliate against cyber attacks by other means. CYBERCOM and other relevant entities also might consider developing a portfolio of cyber tools that are specifically tailored to signaling capabilities and intent.

  - Signal to Tehran that it intends to hold the Iranian government accountable for the actions of its proxies in cyberspace.

  - Recognize that Tehran has legitimate cyber security concerns and include an element of give-and-take in its deterrence strategy.

Introduction

In the face of increasing sanctions, cyber attacks on its nuclear infrastructure, and targeted assassinations of its nuclear scientists, Iran has lashed out against its adversaries, using a variety of kinetic and non-kinetic means. Computer network operations have figured prominently in this regard. Over the past several years, numerous distributed denial of service (DDoS), web defacement, spear phishing, and data manipulation attacks against U.S. and allied networks have been attributed to Iran or its proxies. Iran's cyber targets have included banks, media outlets, government offices, social networking sites, energy companies, individual government officials, and even the Navy Marine Corps Intranet (NMCI). The Iranian regime has also been developing an extensive array of entities and organizations with cyber roles and missions, nominally overseen by the Supreme Cyberspace Council, and integrating cyber drills into its passive defense efforts. Iran's capabilities in the cyber realm, although modest by comparison to first-tier cyber powers such as Russia or Israel, are growing, as evidenced by the increasingly systematic and sustained efforts employed by Iran's cyber forces and the scope of their targets. Tehran has also demonstrated a growing propensity to countenance offensive cyber operations against its adversaries in situations short of actual war.

While Iran's activities in the cyber realm are hardly surprising—the concept of offensive cyber dovetails nicely with the regime's emphasis on asymmetric warfare and its preference for non-attributable means of striking its adversaries—they nevertheless pose critical questions for U.S. entities with cyber roles and missions. Can Iran be deterred from engaging in offensive cyber? If so, how? What would a deterrence strategy that targets Iran's use of offensive cyber look like? Should such a strategy be tailored to deal specifically with Iran?

Various authors have written about the concept of deterrence and how it might be adapted to the cyber realm. When we think about deterrence, the Cold War concept of mutually assured destruction (MAD) usually comes to mind. However, at its most essential level, deterrence involves altering an adversary's actions or behavior by influencing their strategic calculus. The process is, by its very nature, subjective and psychological. It involves getting inside the adversary's decision-making loop, which in turn necessarily entails understanding the various factors that influence the adversary's decision-making processes and perceptions. During the Cold War, the concept was adapted and applied by a great number of theorists to deterring Soviet aggression against the backdrop of the nuclear issue. Today, given the multiplicity and variety of hostile actors in the cyber realm and their contradictory motivations, a one-size-fits-all approach to cyber deterrence—one that does not take into account the unique features of individual adversaries—is unlikely to be effective.

This paper explores an alternative option, based on the concept of tailored deterrence. It employs a case-studies approach to "reconnoiter" a particular adversary—Iran—in order to assess how Iran might be deterred from engaging in certain activities in the cyber sphere. It analyzes some of the unique features associated with the regime's political and military decision making processes, how its cyber programs and entities are structured and affiliated with it, what tactics, techniques, and procedures (TTP) these entities employ, what relative capabilities they have, and how these factors could play in a cyber deterrence scenario. The paper does not attempt to assess the general applicability of the concept of deterrence to the cyber realm. This question has been debated extensively elsewhere. Suffice it to say that the paper starts with the premise that the Iranian regime is a rational actor and therefore can, at least theoretically, be deterred in the cyber realm.

Definitions

Before we begin, I should define what I mean by *offensive cyber* and what kinds of actions by Iran in the cyber sphere should be considered for deterrence. The National Research Council has defined *cyber attacks* as "deliberate actions to alter, disrupt, degrade, or destroy computer systems or networks and the information and/or programs resident in or transiting these systems or networks."[1] This is a good definition for the offensive component of the cyber operations triad, the other elements of which include cyber defense and network exploitation. Offensive cyber operations and network exploitation are often conflated in the press, but the two are quite distinct. While the objective of the former is to degrade a network, affecting the availability and integrity of the information on that network, the latter seeks to exploit the information on a network, affecting its confidentiality. Network exploitation, which is really a form of cyber espionage, could involve stealing information, monitoring network traffic, or conducting reconnaissance on the network to assess its vulnerabilities. In the case of reconnaissance, it could be a precursor to offensive cyber,[2] but it nevertheless retains its distinctive characteristics.

[1] Quoted in P.W. Singer and Allan Friedman, *Cyber Security and Cyber War: What Everyone Needs to Know* (Oxford: University Press, 2014), 64.

[2] The military defines this aspect of cyber operations as "Cyber Operational Preparation of the Environment (C-OPE): Non-intelligence enabling functions within cyberspace conducted to plan and prepare for potential follow-on military operations. C-OPE includes but is not limited to identifying data, system/network configurations, or physical structures connected to or associated with the network or system (to include software, ports, and assigned network address ranges or other identifiers) for the purposes of determining system vulnerabilities; and actions taken to assure future access and/ or control of the system, network, or data during

I would argue that network exploitation is difficult, if not impossible to deter. It occurs on a routine basis, and is conducted by numerous state and non-state actors, ranging from police forces and intelligence agencies to cyber criminals and hacktivist groups, such as Anonymous. It has become so pervasive that the only way to really deter its use is through "deterrence by denial," essentially mounting a good defense. Cyber defense would make even less sense as the object of a deterrence strategy. Within reason, it would be next to impossible to deter Iran from defending itself in the cyber sphere. Nor are we likely to consider such behavior as objectionable in any sense. This paper focuses on the third category, cyber attacks, although I employ the term *offensive cyber*, both for issues of readability and because I think it better conveys the intended meaning.

The fractious nature of the Iranian regime potentially raises the risk of escalation and could complicate U.S. response options.

There is ample evidence to suggest that the Iranian regime is a rational actor—at least rational within the scope of its perceived interests. In other words, we can count on the regime to engage in cost-benefit analysis, and, based on its calculations, act in its own self-interest. Thirty years into its existence, the Islamic Republic is fairly stable and shows no signs of wishing to self-destruct. This would seem to be a prerequisite for deterring any adversary. However, the decentralized nature of the regime suggests that there is a greater risk of escalation in the cyber sphere than would be the case with an adversary with more centralized and streamlined decision making processes.

The political system in Iran is essentially a decentralized oligarchy, with multiple competing centers of power and cross-cutting lines of authority, both formal and informal. While the Supreme Leader is the top decision-maker and ultimate arbiter, he nevertheless tends to rule by consensus, mediating between the various formal and informal power centers in the regime. On contentious national security issues, such as the ongoing nuclear negotiations with the P5+1 or the decision to seek an armistice in the Iran-Iraq War, competition within the system has tended to produce alternating bouts of indecision and over-reaction, as the various power centers in the

anticipated hostilities." Vice Chairman of the Joint Chiefs of Staff Memorandum, "Joint Terminology for Cyberspace Operations: Attachment One, Cyberspace Operations Lexicon," n.d. Accessed at http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

regime seek to outcompete their opponents and appear more loyal to the underlying ideological principles of the Islamic Republic.

At a more granular level, these dynamics are also likely to affect decision-making within those entities that are responsible for conducting offensive cyber operations on behalf of the regime. Most of Iran's cyber-related entities appear to reside in the armed forces and the security services—the Islamic Revolutionary Guard Corps (including the Basij), the regular military, the Ministry of Intelligence and Security (MOIS), and the police. Nominally, the Supreme Cyberspace Council (*shora-ye ali-e fazaye majazi*), which was established by the Supreme Leader in 2012, exercises strategic oversight over all of Iran's cyber activities. The council's members include the country's president, the speaker of the parliament, the head of the judiciary, the commander of the Islamic Revolutionary Guard Corps, the head of the police, the Supreme Leader's representative on the country's Supreme National Security Council, and officials in charge of state broadcasting, information technology, and science. The council acts as a policy-making and an advisory body on cyber related issues. It reports directly to the Supreme Leader, Ayatollah Ali Khamene'i.[3] The Armed Forces General Staff also has its own cyber-related decision making body, the Cyber Defense Command (*gharargah-e defa-e sayberi*), which falls within the purview of the General Staff's Passive Defense Organization.

Theoretically, as commander-in-chief, the Supreme Leader exercises direct control over all of Iran's armed forces, its security services, and the police. In practice, however, his decision-making style has been somewhat passive and indirect—he prefers to rule by consensus, and defers to key leaders and power centers on particular issues. On issues related to Iraq and Syria, for instance, he has tended to defer to General Qasem Soleimani, the commander of the Qods Force.[4] At times, he has encouraged the different services to compete with one another and with the civilian branches of government.[5] As a result, different entities within the military and security services have occasionally acted at cross purposes. Some elements, such as the Qods Force—which may have a cyber role—appear to function more or less autonomously, with little oversight.[6] Various elements within the IRGC and the Basij

[3] BBC Persian, "Structure of Iran's Cyber Warfare." Accessed at http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf.

[4] See, for instance, Dexter Filkins, "The Shadow Commander," *The New Yorker* (30 September 2013). Accessed at http://www.newyorker.com/magazine/2013/09/30/the-shadow-commander.

[5] For instance, various commanders within the IRGC have been openly contemptuous of President Rouhani's attempts to negotiate with the P5+1 over Iran's nuclear program.

have also periodically gotten ahead of the regime on critical issues and been forced to backtrack.

While we have little evidence to suggest how decisions are made within the cyber realm, given the numerous entities involved, we can assume that similar decision-making dynamics are likely to apply. While there will probably be some degree of coordination between the various entities, some organizations are likely to operate at cross purposes with varying degrees of autonomy and possibly with different objectives. Moreover, the potential for escalation is likely to be exacerbated in a cyber exchange, not only because of the compressed nature of time—cyber attacks take place almost instantaneously (although the effects are often not immediately apparent)—but also because the effects of a cyber weapon, once employed, are often difficult to predict. Malware, for instance, can spread beyond its intended target to affect other networks, with no regard for the nature of the network or even national borders.

Tehran perceives that it has been the victim of unjustified cyber aggression by the United States and its allies.

In June 2010, a highly sophisticated version of a worm was discovered embedded in the industrial control systems of Iran's nuclear enrichment center at Natanz. The worm was designed specifically to target the programmable logic coordinators associated with Iran's nuclear centrifuges, causing the centrifuges to operate inefficiently and wear down prematurely. Later dubbed "Stuxnet," the worm was able to infect Iran's nuclear network despite the fact that the network was effectively air-gapped (i.e., not connected to the internet). Designed to be spread via portable thumb drives, it had probably existed for several years on the networks at Natanz before it was detected on foreign networks by the small Belarussian computer security firm VirusBlockAda.[7] Another, more prominent security firm, Kaspersky Lab, conducted extensive forensics analysis on Stuxnet and concluded that it could only have been created with "nation-state support."[8] Subsequent Western media reports claimed that

[6] See, for example, Charlie Savage and Scott Shane, "Iranians Accused of a Plot to Kill Saudis' U.S. Envoy," *New York Times*, 11 October 2011, which describes the Qods Force's role in the so-called Arbabsiar plot.

[7] Paulo Shakarian, *An Introduction to Cyber Warfare: A Multidisciplinary Approach* (New York: Elsevier, 2013), 224.

[8] http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm.

Stuxnet was part of a joint U.S.-Israeli effort, codenamed Olympic Games, which was aimed at sabotaging Iran's nuclear program.[9]

Stuxnet was followed by two even more sophisticated examples of malware—Duqu and Flame—which shared many similarities with Stuxnet in terms of structure,[10] but were evidently focused on collecting information about Iranian industrial control systems associated with Iran's nuclear program and other entities (network exploitation as opposed to offensive cyber).[11] Like Stuxnet, Duqu and Flame have also been attributed to U.S. and Israeli intelligence agencies. Although Stuxnet appears to have had only a limited effect on Iran's nuclear program,[12] its employment was nevertheless a milestone, in that it was the first time that a nation state had used a cyber weapon to offensively target another nation's critical infrastructure. Admiral Michael Hayden, the former CIA chief, claimed in an interview that Stuxnet had "crossed the Rubicon."[13]

Not surprisingly, Iranian officials claimed that Iran had been the victim of an unprovoked attack. Gholam Reza Jalili, the head of Iran's Passive Defense Organization, went so far as to claim that the United States had "initiated a cyber war (*jang-e saybari*) against Iran."[14] In November, 2010, five months after Stuxnet had

[9] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012. Accessed at http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

[10] For example, the computer security firm Symantec claimed, "Duqu is essentially the precursor to a future Stuxnet-like attack. The threat was written by the same authors, or those that have access to the Stuxnet source code, and the recovered samples have been created after the last-discovered version of Stuxnet. Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party." "W32.Duqu: The Precursor to the Next Stuxnet," *Symantec Security Response*, 23 November 2011.

[11] Iranian officials also claimed that their nuclear program had been attacked by an additional virus, dubbed "Stars," in April 2011, which they initially attributed to the United States and Israel. International experts remained skeptical, however, and absent third party forensic analysis, references to Stars in Iranian media have gradually disappeared. See Thomas Erdbrink and Joby Warrick, "Iran: Country under Attack by Second Computer Virus," *Washington Post*, 25 April 2011. Accessed at http://www.washingtonpost.com/world/iran-country-under-attack-by-second-computer-virus/2011/04/25/AFudkBjE_story.html.

[12] Official U.S. government estimates say the effort was set back by 18 months to two years. Sanger, Op. Cit.

[13] Ibid.

[14] "The Head of the Passive Defense Organization: America Has Initiated a Cyber War Against Iran," Iran Student News Agency, 11 May 2014. Accessed at http://www.isna.ir/fa/news/93022113792/

been discovered, General Hossein Hamadani, the head of the IRGC's Rasoulollah (Greater Tehran) division announced that 1,500 Basijis had been trained as "cyber commandos." Hamadani's announcement was significant, not only for its timing, but also for Hamadani's identity: Hamadani was previously a high ranking commander within the Qods Force—the branch of the IRGC in charge of external operations—and would subsequently be one of the primary Qods Force officers in charge of operations in Syria during that country's civil war.

Hamadani's announcement presaged a series of offensive cyber operations against U.S. and allied targets by hacker groups affiliated with Iran. In February, 2011, a group claiming to be the Iranian Cyber Army (ICA) attacked the Voice of America (VOA) website by hijacking the website's domain name. In July and August, 2012, another Iranian-affiliated group, the Cutting Sword of Justice, attacked the networks of the Saudi oil company ARAMCO and the Qatari gas company RasGas with the Shamoon virus, disabling 30,000 computers in the case of ARAMCO.[15] One month later, a group calling itself the Izz al-Din Qassam Cyber Fighters launched a wave of denial of service (DDoS) attacks against major U.S. banks, including including Bank of America, Citigroup, JP Morgan & Chase, and Wells Fargo.[16] Additional attacks by Iranian cyber proxies followed, on U.S. banks (January, March, and May 2013), NASA (June, 2013), and the U.S. Navy (September 2013). Reza Taqipour, the Iranian Minister of Information and Technology, while deflecting blame for the attacks also appeared to offer a justification: "Of course, we do not expect anything more from western countries. This is while we have, from time to time, been subject to state terrorism and cyber attacks on our facilities during the Stuxnet and Flame sagas which were orchestrated by western countries."[17]

Most of these attacks, with the exception of the Shamoon virus, were relatively unsophisticated. Disabled websites were usually restored within a matter of hours. Nevertheless, they appear to have heralded a "new norm" in cyber relations between Iran and the West. Although the pace of attacks has ebbed and flowed, that a low level cyber conflict has been initiated, it is difficult to return to the status quo ante. Essentially, as one report noted, the genie is now "out of the bottle."[18]

---

[15] The attacks on ARAMCO and RasGas may have been partly in response to an unattributed network attack on Iran's Oil and Gas Ministry, which occurred in April 2012.

[16] U.S. officials blamed Iran directly for the DDoS attacks on U.S. banks. Nicole Perlroth and Quentin Hardy, "Bank Hacking Was the Work of Iranians," *New York Times* (8 January 2013).

[17] Mehr News Agency, 31 October 2012. Accessed at http://www.mehrnews.com/detail/News/1733286

[18] Pete Warren, "State-Sponsored Cyber Espionage Projects Now Prevalent, Say Experts," *The Guardian* (30 August 2012). Accessed at http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent.

Iranian officials are likely to define *offensive cyber* differently than we do.

The growth and spread of the internet and the concomitant rise of cyber as an additional domain of warfare have presented Iran with a double-edged sword. On the one hand, Iran has been able to level the playing field somewhat with this new domain, which has a low barrier to entry, particularly for developing nations with a skilled and well-educated work force such as Iran. Also, although the United States undoubtedly possesses very sophisticated offensive cyber capabilities, its openness and its dependence on technologies associated with the internet renders it acutely susceptible to offensive cyber operations. As Admiral Mike McConnell, the former director of national intelligence (DNI), noted, "Because we are the most developed technologically—we have the most bandwidth running through our society and are more dependent on that bandwidth—we are the most vulnerable."[19] Cyber, as a domain of warfare, therefore dovetails nicely with the regime's emphasis on asymmetry. It plays to some of Iran's strengths while exploiting a principal weakness of its adversaries, who are regarded as overly dependent on technology.[20]

On the other hand, the authoritarian nature of the regime renders it acutely susceptible to the free flow of information. In the wake of domestic unrest following the 2009 presidential election in Iran and the subsequent crackdown on pro-democracy protestors, the United States and its allies reached out to dissident groups in Iran, providing training and technology to enable them to circumvent Iran's strict censorship controls and evade detection. Iranian activists rely heavily on virtual private networks (VPNs) and anonymizers, such as TOR, to bypass internet restrictions and hide their identities. Due to the potential for domestic unrest, the Iranian regime regards such technologies—and efforts by the United States and its allies to disseminate their use within Iran—as a major security threat. In this regard, the regime is likely to fear TOR and other examples of U.S. "soft power" more than U.S. conventional capabilities.

In order to counter the threat posed by information technology, the Iranian parliament passed laws that made it a criminal offense to use VPNs and anonymizers, and to access certain social-networking sites, such as Facebook and Twitter. They also established a special branch of the police, the FATA (*faza-yi tawlid va tabadal ettela'at*— or "space for the creation and exchange of information") that is

[19] Quoted in Richard Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Harper Collins, 2010), 145.

[20] See Michael Connell, "Iran's Military Doctrine," in Robin Wright, ed., *The Iran Primer* (Washington, D.C.: USIP, 2010).

responsible for dealing with domestic cyber-related issues. FATA works closely with the Basij and the IRGC, periodically engaging in cyber crackdowns and arresting offending individuals. During one major sweep in 2014, FATA closed 67 internet cafés in Tehran, presumably for allowing their customers to violate internet restrictions.[21] FATA and various components of the IRGC also periodically arrest cyber "criminals" and "agents of foreign powers." To combat the pervasive use of Western social media, the regime has launched alternative, approved versions of websites such as Facebook and YouTube.[22] The regime also leverages cyber proxies, such as the ICA, to target opposition websites.

Given the regime's sensitivities to internal meddling and Western soft power projection, previous attempts by U.S. administrations to facilitate information flow in Iran are probably regarded as a form of offensive cyber—which, when coupled with the targeted cyber attacks on its nuclear program, compounds the perception that Washington is using cyber to undermine the regime. It also suggests that any attempts to deter escalation in the cyber realm will have to take into account that Iranian decision-makers are likely to have a different perception of what constitutes offensive cyber than their U.S. counterparts.

Iran's use of cyber proxies, while hardly unique, adds another layer of complexity to the problem of attribution. It could also have unintended consequences in terms of escalation management, particularly in a crisis scenario.

The Iranian regime periodically leverages the capabilities of domestic and foreign hacker groups—hacktivists—with varying degrees of affiliation to the government, the military, and the private sector in Iran. These groups can be considered proxies for the regime in the cyber sphere in much the same way that armed militias, such as Lebanese Hizballah and Asa'ib Ahl al-Haqq, are in a more traditional military sense. Although motivated by a mix of ideological and sectarian factors, these groups have demonstrated a tendency to coordinate their operations in support of the regime by attacking the networks of regime opponents and adversaries within Iran and abroad.[23]

[21] See http://www.citna.ir

[22] The official alternatives to Facebook and YouTube are Borjface and Aparat, respectively.

[23] How and where these domestic and foreign political hacker groups tie into Iran's military and security services is not clear. It is possible that some of the groups, particularly the foreign ones, coordinate their actions through the IRGC's Qods Force, which is responsible for waging

Initially, the IRGC and other state institutions were slow to leverage the capabilities of non-state actors in the cyber sphere. While Stuxnet and other state-sponsored network attacks on Iranian infrastructure undoubtedly hastened this trend, it was the activities of domestic hacker groups that initially captured the regime's attention. Iran's youth tend to be well educated and tech-savvy. Not surprisingly, therefore, hacking is a well-established tradition in Iran. Iranian hacker groups, which coalesced and mushroomed in the early to mid 2000s, began attacking websites in support of various political or social causes, or simply to compete with one another in order to demonstrate their technical prowess. As the number of attacks on government websites increased, the regime attempted to turn a potential threat into an opportunity by coopting some of these groups and harnessing their capabilities to support the regime through a combination of positive and negative incentives.[24] Private companies were established to recruit professional hackers and teach hacking methods to the armed forces,[25] and government universities with large computer science departments, such as Sharif University of Technology, began to hold hacking competitions to identify potential recruits.[26] Dr. Hassan Abbasi, as well-known IRGC strategist and theorist, was appointed to head the Basij Cyber Council, one of whose functions is to identify rising talent in universities.[27] Once identified, individuals were offered lucrative contracts to work on behalf of the government and, according to one report, threatened with imprisonment if they refused to participate.[28]

Two of the most prominent of these domestic pro-government hacktivist groups are the Iranian Cyber Army (ICA) and Ashiyaneh. ICA was established in the wake of the 2009 election unrest in Iran, when it began attacking domestic Iranian websites affiliated with the Green Movement. Several high-profile external attacks followed, including one that temporarily defaced Twitter in several countries (19 December 2009); another that brought down Baidu, the largest Chinese search engine, on 12 January 2010; and a third that disabled Voice of America's news website,

unconventional warfare against Iran's enemies outside of the country's borders. It also possible that some, particularly the domestic groups, are affiliated with the Basij, given that organization's heavy presence on Iranian university campuses. Regardless of the nature of their affiliation with the Iranian government, it is clear that they coordinate operations and share TTP with each other.

[24] Ashley Wheeler, "The Iranian Cyber Threat." Accessed at http://www.phoenixts.com/blog/the-iranian-cyber-threat/.

[25] Ibid.

[26] Tehran Student News Agency, 26 August 2013.

[27] BBC Persian, "Structure of Iran's Cyber Warfare." Accessed at http://nligf.nl/upload/pdf/Structure_of_Irans_Cyber_Operations.pdf.

[28] Wheeler, "Iranian Cyber Threat."

VOAnews.com, in February 2011. Unlike some of the other Iranian pro-government hacktivist groups, the Iranian Cyber Army is openly affiliated with the IRGC, and may, in fact, fall within that organization's chain of command.[29]

Ashiyaneh, whose moniker means *nest,* has been one of the most prolific Iranian hacker groups, attacking thousands of sites in Europe, the Middle East, Asia, and North America. Headed by Behrouz Kamalian, Ashiyaneh has a business affiliate, Ashiyane Security Center, with its own website (ashiyanehost.com) and training portal.[30] Other significant Iranian pro-government hacktivist groups include Cyber Hizballah, which may be affiliated with the militia arm of the IRGC (the Basij), the Free Cyber Group, the Islamic Cyber Resistance Group, Izz ad-Din al-Qassam Cyber Fighters, Parastoo (*swallow*), and Shabgard (*shadow guard*).[31]

According to a recent Hewlett Packard Security Research report on Iranian pro-government hacker groups and their activities, most of the groups that fit this profile share the following traits: "Their primary language is Farsi, they are heavily influenced by Islamic doctrine, they view Western entities and Israel as enemies, they use a combination of technical and non-technical tactics to exploit targets, they make their exploits known publicly via social media or the zone-h leaderboard, and their key members are well educated and well connected…. Additionally, members of the key groups profiled are known to associate with one another, both online and offline."[32]

Outside of the domestic arena, Iranian cyber entities appear to be leveraging, or at least coordinating, some of their efforts with foreign hacktivists with whom they share political and ideological goals—mainly Shia Islamist hacker groups in the Middle East. The most prominent of these is the Syrian Electronic Army (SEA), which has been very active in targeting U.S., Israeli, and Gulf Cooperation Council cyber infrastructure. The group, which has declared its loyalty to Syrian President Bashar Al-Assad, a key ally of Iran, was recently labelled "an extension of the Iranian State" by General Michael Hayden, former director of the CIA and the NSA.[33] In 2013, the

[29] Various IRGC officials have referred to the "Cyber Army" (*artesh-e saybari*) as an IRGC affiliate. See, for instance, "Sepah's Cyber Army is Considered the Second in the World," Fars News, 20 May 2010. Accessed at http://www.farsnews.com/newstext.php?nn=8902300353, which includes a photo with the Iranian Cyber Army's banner from a website defacement.

[30] *HP Threat Intelligence Briefing*, Episode 11, February 2014.

[31] See *HP Threat Intelligence Briefing*, Episode 11, February 2014 for more details.

[32] Ibid.

[33] Carlo Munoz, "Hayden: Pro-Syrian hacker group working with Iran," *The Hill* (21 November 2013). Accessed at http://thehill.com/policy/defense/191132-hayden-pro-syrian-hacker-group-working-with-iran.

SEA garnered considerable media attention when it hijacked the Associated Press's Twitter account and claimed that the White House had been attacked and that President Obama had been injured. The message briefly spooked financial markets, causing stock prices to tumble temporarily.[34] Other major actors in what could be termed the *Shia cyber crescent* include Lebanese Hizballah and the Iraqi Shia militias Asa'ib Ahl al-Haq and Kata'ib Hizballah, all of which have conducted offensive cyber operations, primarily against Israeli and Salafi-jihadist networks.

Iran's military and security services leverage cyber proxies such as Ashiyaneh and SEA to bolster their capabilities while affording the regime a degree of plausible deniability in its operations. This fact can further exacerbate the already complex issue of attribution in the cyber realm. Cyber attacks rarely result in a "smoking gun," where the perpetrator can be positively identified beyond any doubt. Hackers, for instance, will often use third-party networks (botnets), which they have coopted unbeknownst to their users, to conduct operations. Botnets could be located—and frequently are—in countries other than those of their operators. Thus, while an IP address might provide some indication as to the vector of an attack, it says little about its origins.

As they do in the conventional realm, proxies add another layer of complexity to the issue of attribution in the cyber context with potential implications for escalation management. Assuming that the initiators of an attack can be identified—either due to forensics analysis or perhaps because the hackers brag about their successes in internet fora—is it safe to assume that the hackers acted on behalf of their respective state sponsors? Cyber surrogates—like other, more traditional, proxies—do not always operate in concert with their patrons. While the activities of the groups listed above appear to suggest a high degree of cooperation and coordination with the Iranian government, a few of their actions would, at least at face value, appear to run counter to the regime's interests, suggesting that they have some latitude for independent action.

For instance, on January 12, 2010, ICA hackers paralyzed China's largest search engine, Baidu, by hijacking the site's domain name and redirecting its traffic to an alternate website. The attack sparked a brief spate of retaliations between Chinese and Iranian hackers, and left many puzzled about why ICA would attack the website of one of Iran's allies, especially in light of Iran's attempts to court China in order to offset its political and economic isolation. Some Chinese analysts speculated that ICA's attack might have been motivated by the actions of Chinese Twitter users who

[34] Ibid.

used a #C4NIran hashtag to support Iranian reformers.[35] While this makes sense from a purely tactical perspective, it would seem to undermine the regime's arguably greater strategic and economic objectives. Regardless of the explanation, the attack on Baidu illustrates that groups such as ICA, despite their affiliation with the Iranian regime, sometimes engage in actions that appear to run counter to the interests of their sponsor. In a crisis situation, groups such as ICA or Ashiyaneh could engage in escalatory behavior precisely when the regime might be trying to deescalate the situation. While Iran is hardly unique in the fact that it leverages non-state actors to conduct network attacks,[36] Iran's employment of hacktivists is likely to have implications for any tailored deterrence strategy.

Iranian capabilities are modest but growing.

Although Iran's entry into the cyber sphere was relatively late—IRGC officials first announced their intention to develop a cyber capability in 2005[37]—Iran has rapidly catapulted into the second or third tier of world cyber powers. Prior to 2012, the tactics employed by Iran's cyber forces and their proxies were fairly basic by hacking standards—mainly SQL injects, DDoS attacks with botnets, and DNS hijackings and recursions.[38] In most cases, their hacks did not end up penetrating targeted networks. Either they overloaded a targeted website or they compromised an external system to redirect traffic away from the targeted site. As a result, the impact of their attacks tended to be ephemeral, albeit high profile in many instances.

However, by 2012, Iranian cyber efforts were maturing and becoming more systematic. The first indication of this occurred in September, when the Cutting Sword of Justice—an Iranian proxy—used a cyber weapon, the "Shamoon virus," to incapacitate the networks of energy firms in Saudi Arabia and Qatar. Saudi Aramco was hit particularly hard. More than 30,000 computers in Aramco's commercial

[35] Tania Branagan, "'Iranian' Hackers Paralyse Chinese Search Engine Baidu," *The Guardian* (12 January 2010). Accessed at http://www.theguardian.com/technology/2010/jan/12/iranian-hackers-chinese-search-engine.

[36] For instance, the role of Nashi, a quasi-governmental Russian youth group, in the massive cyber-attacks against Estonia during the week of 27 April 2007 have been well documented. See, for example, Paulo Shakarian, *An Introduction to Cyber Warfare: A Multidisciplinary Approach* (New York: Elsevier, 2013), 19-20.

[37] Wheeler, "Iranian Cyber Threat."

[38] See the HP report for a detailed analysis.

network were disabled by the virus.[39] While not nearly as sophisticated as Stuxnet, the Shamoon virus nevertheless illustrated that Iran's cyber forces were capable of generating more enduring effects than had hitherto been suspected.

In addition to the Aramco attack, two other events suggested that Iranian cyber capabilities were on an upward trajectory—although, strictly speaking, in neither of these instances could the operations mounted by Iran's cyber forces be considered true cyber attacks, rather, they were examples of network exploitation or cyber espionage. In 2013, Iranian hackers managed to penetrate the Navy Marine Corps Intranet (NMCI), the Navy and Marine Corps' principal unclassified communications network. Capitalizing on a weakness in NMCI's public website, hackers remained on the network for four months, exfiltrating account information and other data from the network.[40] The penetration cost the Navy $10 million to patch, and was considered to be particularly invasive.[41]

The NMCI incident was followed shortly afterwards by a sophisticated attempt—dubbed "Newscaster" by the security company that discovered it—to use social networking sites such as LinkedIn and Facebook to target hundreds of U.S. officials and their connections in order to steal log-in and password information and to obtain sensitive information "that could support weapon systems development, or provide insight into the U.S. military, the U.S.-Israel alliance or nuclear negotiations between Iran and the United States and other powers."[42] To support their ruse, the Iranian hackers engaged in an elaborate program of social engineering, creating fake online personas with detailed backgrounds as well as a fake news site—NewsOnAir.org—that featured news stories derived from genuine news sites.

Together, these three operations—the Aramco attack, the NMCI penetration, and Newscaster—have served as a wake-up call to Western defense establishments, alerting them to Iran's growing cyber ambitions, perseverance, and capabilities. While Iran is still well behind the first-tier cyber powers, including the United States, Russia, the UK, and Israel, it is gradually catching up. In part, the efforts of Iran's

[39] Siobhan Gorman, "Iran-Based Cyberspies Targeting U.S. Officials, Report Alleges," *Wall Street Journal* (29 May 2014). Accessed at http://online.wsj.com/articles/iran-based-cyberspies-targeting-u-s-officials-report-alleges-1401335072.

[40] Elliot Jager, "Iranian Hackers Penetrated US Navy Marine Corps Internet for Four Months," *Newsmax* (18 February 2014).

[41] Ibid.

[42] Ellen Nakashima, "Iranian Hackers are Targeting U.S. Officials through Social Networks, Report Says," *Washington Post* (29 May 2014). Accessed at http://www.washingtonpost.com/world/national-security/iranian-hackers-are-targeting-us-officials-through-social-networks-report-says/2014/05/28/7cb86672-e6ad-11e3-8f90-73e071f3d637_story.html.

cyber forces have been bolstered by the burgeoning black market in cyber weapons and vulnerabilities.[43] In the meantime, as a recent Atlantic Council report noted, "Iran does not need the equivalent of a Ferrari to inflict damage on US infrastructure: a Fiat may do."[44]

Outlining the general contours of a strategy to deter Iran's use of offensive cyber

According to the 2010 Quadrennial Defense Review, "Credibly underwriting U.S. defense commitments will demand tailored approaches to deterrence. Such tailoring requires an in-depth understanding of the capabilities, values, intent, and decision making of potential adversaries, whether they are individuals, networks, or states."[45] Implicitly, this approach recognizes that a deterrence strategy is more likely to be successful if it takes into account not just an adversary's capabilities, but also the unique strategic context in which a given adversary operates. It also suggests that a one-size-fits-all approach to deterrence—especially in the cyber realm, given the multiplicity and diversity of actors involved—is unlikely to be effective. As Singer and Friedman have noted in their seminal study *Cyber Security and Cyber War*, "The United States has approached deterrence very differently when facing terrorists, rogue nations, and major powers. While the theory often lays out a series of set

[43] According to a report in *Forbes*, so-called 0-Days—previously unidentified software-hacking vulnerabilities—can typically be bought for between five and six figures. "Each price assumes an exclusive sale, the most modern version of the software, and, of course, not alerting the software's vendor. Some fees might even be paid in installments, with each subsequent payment depending on the vendor not patching the security vulnerabilities used by the exploit. In some cases the techniques would need to be used in combination to be effective." See http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

[44] Barbara Slavin and Jason Healey, *Iran: How a Third Tier Cyber Power Can Still Threaten the United States,* The Atlantic Council (29 July 2013).

[45] *Quadrennial Defense Review Report* (February 2010). Accessed at

http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf. The 2006 *Quadrennial Defense Review Report* also briefly addresses the issue of tailored deterrence, noting that "The Department is continuing its shift from a "one size fits all" notion of deterrence toward more tailorable approaches appropriate for advanced military competitors, regional WMD states, as well as non-state terrorist networks." http://www.defense.gov/qdr/report/Report20060203.pdf

actions and counter actions, the reality is that different actors can dictate very different responses."[46]

This paper has explored the concept of tailored deterrence in the cyber realm from the perspective of a particular adversary—Iran. Based on our analysis of the particular—and in some cases unique—attributes of the Iranian regime, what factors should Washington consider if it were to formulate a strategy to deter Iran's use of offensive cyber? What might a tailored deterrence strategy look like? The following are some of the factors that might inform such a strategy.

- Washington should define what categories of activities in the cyber realm it considers intolerable and would therefore warrant retaliation, and communicate its intent to Iran's leadership via multiple channels. There is some benefit to maintaining a policy of strategic ambiguity concerning cyber "redlines." But given the potential for miscalculation between Iran and the United States, as well as the unpredictable and poorly understood nature of cyber warfare, Washington should define those activities that it considers to be intolerable and signal its intent to respond to provocations that meet this definition. Ideally, this would be done as part of a broader strategic attempt to define international cyber norms and conventions. Absent such a framework, however, Washington should communicate its stance clearly and directly to Iran's leadership via several official channels, given the multiplicity of actors on the Iranian side. The categories would necessarily have to be broad and imprecise, given the diversity of cyber weapons, the sometimes unpredictable nature of their effects, and the fluid nature of the battle space. Putting a lid even on low-level cyber attacks (DDoS, etc.), let alone on examples of network exploitation, will be difficult absent a major shift in the broader strategic environment. Therefore, the strategy should focus on deterring only the more disruptive examples of attack—for instance, those on critical U.S. infrastructure and economic targets.

- A tailored deterrence strategy will have to account for the fact that Iranian officials are likely to define offensive cyber differently than we do. Activities that we might regard as relatively benign—for instance, ensuring the free flow of information across borders—might be regarded as hostile by a regime such as Iran's that places a premium on maintaining domestic security and combatting internal unrest.

[46] Singer and Friedman, *Cyber Security and Cyber War,* 146. The authors go on to note how the U.S. response to the major cyber attacks mounted against Estonia in 2007 might have been very different if the culprit had turned out to be Tehran rather than Moscow.

- Washington should demonstrate that it has a credible means of retaliation in cyberspace, while at the same time declaring that it reserves the right to retaliate against cyber attacks by other means. Mounting an effective defense is an important component of cyber deterrence, but alone it is unlikely deter cyber attacks by Tehran or other potential adversaries, especially given U.S. vulnerabilities in cyberspace and the fact that in this area, the advantage is often weighted in favor of the offense. Until now, cyber attacks by Iran and its proxies have largely gone unanswered. This may have given Iranian decision makers a false and destabilizing sense of security, encouraging additional and possibly more escalatory attacks in the future. In order to mitigate this potential, Washington should demonstrate that it has the means and the will to respond to cyber attacks that fall within the scope of activities outlined above. While demonstration effects are difficult to mount in the cyber realm—some cyber weapons can only be used once—CYBERCOM and other relevant entities might consider developing a portfolio of cyber tools that are specifically tailored to demonstrating capabilities and signaling intent.[47] In assessing its response options should deterrence fail, Washington should think asymmetrically—that is, while a response should be proportional, it need not be restricted to cyberspace. In some cases, a conventional military, economic, or diplomatic response may be warranted, particularly in those areas where the United States has a clear advantage.

- Washington should signal to Tehran that it intends to hold the Iranian government accountable for the actions of its proxies in cyberspace. Iran's cyber forces outsource operations to hacker groups such as SEA and ICA for the same reasons that the Qods Force works with militant groups such as Hizballah: they act as force multipliers, they contribute additional expertise, and they afford the regime a degree of plausible deniability in its operations. While recognizing that such groups do not always act in consort with their sponsor, we should encourage Tehran to keep them in check by holding Iran responsible for their actions.

- In order to be successful, a deterrence strategy would have to recognize that Tehran has legitimate cyber security concerns and include an element of give-and-take. Cyber attacks on Iran's nuclear and commercial infrastructure, coupled with Western attempts to widen the information aperture into Iran, have raised the suspicions of the regime and convinced many Iranian officials that the Islamic Republic is the victim of unjustified cyber aggression by the United States and Israel. In order to successfully deter Iran from launching

[47] Many of the more sophisticated cyber weapons are ill suited to signaling, because they have small signatures. They are often designed to confound detection and avoid attribution.

cyber attacks on U.S. targets, Washington should also refrain from engaging in offensive cyber operations against Iranian networks.

The CNA Corporation

This report was written by CNA Corporation's Strategic Studies (CSS) division.

CSS is CNA's focal point for regional expertise and analyses, political-military studies, and U.S. strategy and force assessments. Its research approach anticipates a broad scope of plausible outcomes assessing today's issues, analyzing trends, and identifying "the issue after next," using the unique operational and policy expertise of its analysts.

DIM-2014-U-008820-Final

CNA Corporation is a not-for-profit research organization
that serves the public interest by providing
in-depth analysis and result-oriented solutions
to help government leaders choose
the best course of action
in setting policy and managing operations.

Nobody gets closer—
to the people, to the data, to the problem.

CNA
ANALYSIS & SOLUTIONS

www.cna.org • 703-824-2000

3003 Washington Boulevard, Arlington, VA 22201